JOURNAL OF NUMBER THEORY 20, 273–281 (1985)

Computing Galois Groups over the Rationals

LEONARD SOICHER*

Department of Pure Mathematics and Mathematical Statistics, 16 Mill Lane, Cambridge, England CB2 1SB

AND

JOHN MCKAY

Department of Computer Science, Concordia University, Montreal, Quebec, Canada H3G 1M8

Communicated by O. Taussky Todd

Received October 22, 1982

DEDICATED TO PROFESSOR HANS ZASSENHAUS

Practical computational techniques are described to determine the Galois group of a polynomial over the rationals, and each transitive permutation group of degree 3 to 7 is realised as a Galois group over the rationals. The exact computations furnish a proof of the result.

1. INTRODUCTION

Let $f = f(x)$ be a polynomial in $Q[x]$, with $\deg(f) = n$, having distinct zeros $a_1, \ldots, a_n$. We regard $\mathrm{Gal}(f)$, the Galois group over the rationals, to be the group of permutations of the (indices of the) zeros of f induced by the group of automorphisms of the splitting field, $\mathrm{spl}(f)$, of f.

In van der Waerden [16, p. 189] a finite procedure to determine $\mathrm{Gal}(f)$ is described. This procedure requires the construction and factorization of a degree $n!$ polynomial and thus it is not suitable for practical purposes. In this paper we describe feasible computational techniques to determine $\mathrm{Gal}(f)$. The aim is to efficiently determine sufficient properties to specify $\mathrm{Gal}(f)$ to within conjugacy in the symmetric group S_n of degree n. This conjugation is realised by relabelling the zeros of f. We consider only irreducible f so that $\mathrm{Gal}(f)$ is transitive and assume without loss of generality that f is monic with integer coefficients.

A well-known method of determining cycle types in $\mathrm{Gal}(f)$ is the follow-

* This research is supported by NSERC and FCAC funding.

0022-314X/85 $3.00

ing [16, p. 191]: for a prime p not dividing disc(f), the discriminant of f, the partition of n induced by the degrees of the irreducible factors of f modulo p (called the degree partition of f mod p) is the cycle type of a permutation in Gal(f).

In fact, by the density theorem of Chebotarev (see [7]), as $k \to \infty$, the proportion of occurrences of a degree partition T of f mod p_i, $i = 1,..., k$ (p_i the ith prime) tends to the proportion of permutations in Gal(f) having cycle type T; but the full power of this result seems difficult to use in practice.

Butler and McKay [2] have tabulated the transitive permutation groups of degree up to 11, and the cycle type distribution of permutations in these groups. After f is factorized modulo various primes, these tables are used to obtain a set of groups $\{H_i\}$ such that $\forall i$, $H_i \not\supseteq$ Gal(f). In fact, if Gal(f) is A_n or S_n (A_n is the alternating group on $\{1,..., n\}$), then Gal(f) can usually be quickly determined using modulo p factorizations and the fact that Gal(f) is a group of even permutations if and only if disc(f) is a rational integral square. If Gal(f) is neither A_n nor S_n, an historical and very useful method to determine Gal(f) is the construction and factorization of appropriate resolvent polynomials.

2. Resolvent Polynomials

Let $F = F(x_1,..., x_n)$ be a polynomial in $Z[x_1,..., x_n]$ and let P be a permutation in S_n. We define $F^P = F(x_{1P},..., x_{nP})$. In this way any subgroup of S_n acts on $F^{S_n} = \{F^P : P \in S_n\}$.

Definition 1. Let $\{F_1,..., F_k\} = F^{S_n}$, where the F_i are distinct functions. The resolvent polynomial $R(F, f)$ associated with F and f is defined by

$$R(F, f) = \prod_{i=1}^{k} (x - F_i(a_1,..., a_n)).$$

We may take $F_i = F^{P_i}$, $1 \leqslant i \leqslant k$, where $\{P_1,..., P_k\}$ is a set of right coset representatives of $\text{stab}_{S_n}(F)$ (the stabilizer in S_n of F) in S_n.

Definition 2. A resolvent polynomial $R(L, f)$, where $L = e_1 x_1 + \cdots + e_r x_r$, for some r, $1 \leqslant r \leqslant n$, and $e_1,..., e_r$ nonzero integers, is called a *linear resolvent polynomial.*

The coefficients of a resolvent polynomial $R(F, f)$ are algebraic integers which are symmetric functions of the zeros $a_1,..., a_n$ of f, hence these coefficients are rational integers. We shall now assume throughout that the zeros of $R(F, f)$ are distinct, for if not, we may apply an appropriate

Tschirnhaus transformation to f preserving the Galois group, then recompute $R(F, f)$.

$\mathrm{Gal}(f)$ acts on the set of zeros of $R(F, f)$ by permuting the $\{a_i\}$. As the zeros of $R(F, f)$ are distinct this action is equivalent to the action by $\mathrm{Gal}(f)$ on F^{S_n}. The orbits of the action by $\mathrm{Gal}(f)$ on the zeros of $R(F, f)$ are precisely the sets of zeros of the distinct irreducible factors (over Q) of $R(F, f)$.

For a group G acting on a finite set S we call the partition of $|S|$ induced by the lengths of the orbits of S under G the *orbit-length partition* of S under G. Thus we have

PROPOSITION 1. *The orbit-length partition of* F^{S_n} *under* $\mathrm{Gal}(f)$ *is the same as the partition of* $\deg(R(F, f))$ *induced by the degrees of the irreducible factors of* $R(F, f)$.

The resolvent polynomial $R(F, f)$ can be constructed by expanding $R(F, f)$ symbolically in the zeros of f and then determining the coefficients of $R(F, f)$ as polynomials in the coefficients of f. Unfortunately, unless $\deg(R(F, f))$ is small or f is sparse, this leads to very extensive symbolic manipulation. However, if we use this method, we get an explicit formula for the coefficients of $R(F, f)$ in terms of the coefficients of f. Such formulae have been published for certain resolvent polynomials in [1, 4, 5, 11].

$R(F, f)$ can also be formed using high-precision numerical approximations to the zeros of f. If the coefficients of $R(F, f)$ are determined to within an absolute error less than $\frac{1}{2}$, then these coefficients are determined exactly by rounding. Stauduhar [14] employs this method.

The results presented here form part of the first author's Master's thesis [13] in which he details a new, practical, exact algorithm to construct linear resolvent polynomials. This algorithm does not expand the resolvent symbolically in the zeros of f.

To factorize $R(F, f)$ we use Hensel's method (see [17]). Alternatively, one can often determine candidates for factors of $R(F, f)$ by using numerical approximations to the zeros of $R(F, f)$.

Often (see, e.g., [1, 6, 9, 14],) resolvent polynomials are used to determine if $\mathrm{Gal}(f)$ is contained in some given proper subgroup G of S_n. If F is chosen so that $G = \mathrm{stab}_{S_n}(F)$, then $R(F, f)$ has a linear factor if and only if $\mathrm{Gal}(f)$ is contained in some conjugate of G in S_n. Although linear factors are easy to find, they give information only about the Galois group's containment in one group and its conjugates. The complete factorization of a well-chosen resolvent polynomial can often determine $\mathrm{Gal}(f)$ among possible candidates.

3. Linear Resolvent Polynomials

Linear resolvents form a general class of useful resolvent polynomials for $f(x)$ of any degree. Often the factorization of linear resolvents of relatively low degree can be used to determine Gal(f). We may use linear resolvents to determine the orbit-length partition of r-sets or r-sequences under Gal(f) ($1 \leqslant r \leqslant n$).

A subgroup G of S_n acts on the $\binom{n}{r}$ r-sets contained in $\{1,..., n\}$, where the action is defined by $\{i_1,..., i_r\}^P = \{i_1 P,..., i_r P\}$ for all $P \in G$. Now let $L = x_1 + \cdots + x_r$. It is clear that the action of G on L^{S_n} is equivalent to the action of G on the r-sets contained in $\{1,..., n\}$. Thus the factorization of $R(L, f)$ determines the orbit-length partition of r-sets under Gal(f). Erbach, Fischer, and McKay [5, 10] suggest using resolvents of this type in order to determine the transitivity of Gal(f) on r-sets. The following remark is of interest: for f irreducible and $n = rs$, $r, s \neq 1$, $R(L, f)$ has t irreducible factors of degree s if and only if Gal(f) has t systems of imprimitivity of s blocks of size r.

A subgroup G of S_n acts on the $n!/(n-r)!$ r-sequences of distinct elements of $\{1,..., n\}$ where the action is defined by $(i_1,..., i_r)^P = (i_1 P,..., i_r P)$ for all $P \in G$. Now let $L = e_1 x_1 + \cdots + e_r x_r$, where $e_1,..., e_r$ are *distinct* nonzero integers. Now suppose $R(L, f)$ has distinct zeros, then $R(L, f)$ is reducible if and only if Gal(f) is not r-ply transitive. There is also a simple field-theoretic interpretation to the factorization of $R(L, f)$. Let $b = e_1 a_{1P} + \cdots e_r a_{rP}$, $P \in S_n$, be a zero of $R(L, f)$. We see that

$$\mathrm{stab}_{\mathrm{Gal}(f)}(b) = \bigcap_{i=1}^{r} \mathrm{stab}_{\mathrm{Gal}(f)}(a_{iP});$$

hence $Q(b) = Q(a_{1P},..., a_{rP})$. The degrees of the irreducible factors of $R(L, f)$ correspond to the degrees over Q of nonconjugate subfields of spl(f) generated by r-sets of the zeros of f. For irreducible f and $r = 2$, we note that $R(L, f)$ has irreducible factors all of degree n if and only if $Q(a_i) = Q(a_j)$ for all $1 \leqslant i, j \leqslant n$ if and only if spl(f) $= Q(a_i)$ for all $1 \leqslant i \leqslant n$ if and only if Gal(f) is a regular permutation group. We also note that if $r = n-1$ or $r = n$, then $R(L, f)$ has degree $n!$ and spl(f) $= Q(b)$ for each zero b of $R(L, f)$.

For the transitive permutation groups G of degree 3 to 7, Table I contains the orbit-length partitions of r-sets (r up to $\frac{1}{2}$ degree of G) and 2-sequences (with distinct elements) under G. This table was computed by Butler using the group-theoretical computer language CAYLEY [3]. For irreducible f of degree up to 7, Table I is used to determine candidates for Gal(f) given the factorization of a linear resolvent which determines the orbit-length partition of r-sets or 2-sequences under Gal(f).

TABLE I

Orbit-length Partitions of Sets and Sequences under G

G	2-sets	3-sets	2-sequences
Degree 3			
$+A_3$			3^2
S_3			6
Degree 4			
Z_4	2,4		4^3
$+V_4$	2^3		4^3
D_4	2, 4		4, 8
$+A_4$	6		12
S_4	6		12
Degree 5			
$+Z_5$	5^2		5^4
$+D_5$	5^2		10^2
F_{20}	10		20
$+A_5$	10		20
S_5	10		20
Degree 6			
Z_6	$3, 6^2$	$2, 6^3$	6^5
S_3	$3^3, 6$	$2, 6^3$	6^5
D_6	$3, 6^2$	2, 6, 12	$6, 12^2$
$+A_4$	3, 12	$4^2, 6^2$	$6, 12^2$
G_{18}	6, 9	2, 18	$6^2, 18$
G_{24}	3, 12	$6^2, 8$	$6, 12^2$
$+S_4/V_4$	3, 12	$4^2, 12$	6, 24
S_4/Z_4	3, 12	8, 12	6, 24
G_{36}^1	6, 9	2, 18	12, 18
$+G_{36}^2$	6, 9	2, 18	12, 18
G_{48}	3, 12	8, 12	6, 24
$+\mathrm{PSL}_2(5)$	15	10^2	30
G_{72}	6, 9	2, 18	12, 18
$PGL_2(5)$	15	20	30
$+A_6$	15	20	30
S_6	15	20	30
Degree 7			
$+Z_7$	7^3	7^5	7^6
D_7	7^3	$7^3, 14$	14^3
$+F_{21}$	21	$7^2, 21$	21^2
F_{42}	21	14, 21	42
$+PSL_3(2)$	21	7, 28	42
$+A_7$	21	35	42
S_7	21	35	42

The notation for the group names is similar to that of McKay [10], who gives group generators. A_n is the alternating group of degree n; S_n is the symmetric group of degree n; Z_n denotes the cyclic group of order n; V_4 is the four-group; D_n denotes the dihedral group of order $2n$; F_n denotes a Frobenius group of order n; G_n denotes a group of order n. If A and B are groups then A/B means that A is represented on the cosets of B in A. Groups preceded by "+" are groups of even permutations.

EXAMPLE. Consider $f(x) = x^7 - 14x^5 + 56x^3 - 56x + 22$; $\text{disc}(f) = 2^{67}10^{10}$; f is irreducible over Q. We compute and factorize $R = R(x_1 + x_2 + x_3, f)$ of degree 35 to determine the orbit-length partition of 3-sets under $\text{Gal}(f)$. Factorizing R into irreducible factors over Q, we find that $R = R_1 R_2 R_3$, where

$$R_1 = x^7 - 28x^5 + 224x^3 - 448x + 94,$$

$$R_2 = x^7 - 28x^5 + 224x^3 - 448x + 192,$$

and

$$\begin{aligned} R_3 = {} & x^{21} - 84x^{19} + 2436x^{17} - 31136x^{15} + 6358x^{14} + 203840x^{13} - 84392x^{12} \\ & - 733824x^{11} + 420728x^{10} + 1480192x^9 - 988064x^8 - 1652036x^7 \\ & + 1138368x^6 + 986496x^5 - 620928x^4 - 284032x^3 + 137984x^2 \\ & + 27104x - 10648. \end{aligned}$$

R has distinct zeros and its factorization shows that the orbit-length partition of 3-sets under $\text{Gal}(f)$ is 7^2, 21. From Table I we see that $\text{Gal}(f)$ is F_{21}, the Frobenius group of order 21 on 7 letters.

Remark 1. The ability to compute linear resolvents efficiently [13] allows us to compute certain useful quadratic resolvents. When $R(F, f)$ is a resolvent such that $F^P = -F$ for some $P \in S_n$, we see that $R(F^2, f)(x^2) = R(F, f)(x)$. For example, suppose $\deg(f) = 5$ and $\text{Gal}(f)$ is either F_{20} or S_5. We compute and factorize $R = R((x_1 + x_2 - x_3 - x_4)^2, f)$ of degree 15, using a linear resolvent, to distinguish between these candidates. Now $\text{Gal}(f) = F_{20}$ if and only if R is reducible. In this case R has irreducible factors of degrees 5 and 10.

Remark 2. For $n = \deg(f) = 3$, 4, 5, 7, the conjugacy class in S_n of transitive $\text{Gal}(f)$ is determined completely by the "squareness" of $\text{disc}(f)$ and the orbit-lengths of the action of $\text{Gal}(f)$ on 2-sets, 3-sets, and 2-sequences, with the exception of distinguishing F_{20} from S_5 (but this has been taken care of in Remark 1).

For degree 6, all the transitive groups can be differentiated by $\text{disc}(f)$ and the orbit-lengths on 2-sets, 3-sets, and 2-sequences except to distinguish S_4/Z_4 from G_{48}, G_{36}^1 from G_{72}, and $PGL_2(5)$ from S_6. We briefly

outline a suitable technique to distinguish these groups. We assume that all polynomials discussed have distinct zeros.

Let d be the squarefree part of $\operatorname{disc}(f)$, and $g(x)$ be a monic irreducible factor of a resolvent polynomial $R(F, f)$ such that $F_j(a_1,..., a_n)$ is a zero of g for a specific $F_j \in F^{S_n}$ ($a_1,..., a_n$ the zeros of f). Define $g_d(x)$ to be the monic integral polynomial of degree $2 \times \deg(g)$ having the zeros $b_k \pm d^{1/2}$, where the b_k run through the zeros of g. The following are equivalent:

(1) $\operatorname{stab}_{\mathrm{Gal}(f)}(F_j)$ is a subgroup of A_n.

(2) $Q(F_j(a_1,..., a_n))$ contains $Q(d^{1/2})$.

(3) g_d is reducible (see [16, pp. 126–127]; also see [13] for computational details).

Now suppose $n = 6$ and $R = R(x_1 + x_2 + x_3, f)$ of degree 20.

Suppose $\mathrm{Gal}(f) = S_4/Z_4$ or G_{48}. Let g be the monic irreducible factor of degree 12 of R. Then $\mathrm{Gal}(f) = S_4/Z_4$ if and only if g_d is reducible.

Suppose $\mathrm{Gal}(f) = G_{36}^1$ or G_{72}. Let g be the monic irreducible factor of degree 2 of R. Then $\mathrm{Gal}(f) = G_{36}^1$ if and only if g_d is reducible.

Suppose $\mathrm{Gal}(f) = PGL_2(5)$ or S_6. Let $g = R$. Then $\mathrm{Gal}(f) = PGL_2(5)$ if and only if g_d is reducible.

4. Polynomials with Given Transitive Galois Groups

It is an unsolved problem whether any permutation group can appear as the Galois group of a polynomial over Q. For each solvable group G it is known that there exists a polynomial f such that $\mathrm{Gal}(f) = G$ (see [12]); however there has not yet appeared a practical general method of constructing an f from any given solvable G.

For each transitive permutation group G of degree 3 to 7, we have computed a polynomial $f(x)$ such that $\mathrm{Gal}(f) = G$. These polynomials appear in Table II; z_n denotes a primitive nth root of 1.

For each polynomial f in Table II we have proved that $\mathrm{Gal}(f)$ is the group indicated. Many of the polynomials f are constructed so that $\mathrm{spl}(f)$ is contained in some known field. The methods of doing this include constructing f to be a resolvent polynomial, constructing f to be a composite polynomial, or if $\mathrm{Gal}(f)$ is to be cyclic, by constructing f such that $\mathrm{spl}(f)$ is contained in $Q(z_p)$, p prime. This knowledge about $\mathrm{spl}(f)$ is used to reduce or eliminate the work necessary to determine $\mathrm{Gal}(f)$. The only polynomials whose Galois groups are determined using other information than the splitting field, cycle types, or discriminant are those f with $\mathrm{Gal}(f) = D_5$, D_7, F_{21}, or $PSL_3(2)$. These exceptions are proved to have the group indicated by using the factorization of appropriate linear resolvent polynomials (cf. Table I).

TABLE II

Polynomials $f(x)$ Such That $\mathrm{Gal}(f) = G$

G	$\mathrm{Disc}(f)$	$f(x)$	Remarks
Degree 3			
$+A_3$	7^2	x^3+x^2-2x-1	$\mathrm{spl}(f)=Q(z_7+z_7^{-1})$
S_3	$-2^2 3^3$	x^3+2	
Degree 4			
Z_4	5^3	$x^4+x^3+x^2+x+1$	$\mathrm{spl}(f)=Q(z_5)$
$+V_4$	2^8	x^4+1	$\mathrm{spl}(f)=Q(z_8)$
D_4	-2^{11}	x^4-2	
$+A_4$	$2^{12}3^4$	$x^4+8x+12$	
S_4	229	x^4+x+1	
Degree 5			
$+Z_5$	11^4	$x^5+x^4-4x^3-3x^2+3x+1$	$\mathrm{spl}(f)=Q(z_{11}+z_{11}^{-1})$
$+D_5$	$2^{12}5^6$	$x^5-5x+12$	
F_{20}	$2^4 5^5$	x^5+2	
$+A_5$	$2^{16}5^6$	$x^5+20x+16$	
S_5	19.151	x^5-x+1	
Degree 6			
Z_6	-7^5	$x^6+x^5+x^4+x^3+x^2+x+1$	$\mathrm{spl}(f)=Q(z_7)$
S_3	$-2^{16}3^{21}$	x^6+108	$\mathrm{spl}(f)=\mathrm{spl}(x^3+2)$
D_6	$-2^{11}3^6$	x^6+2	
$+A_4$	$2^6 3^8$	x^6-3x^2-1	$\mathrm{spl}(f)=\mathrm{spl}(x^4+8x+12)$
G_{18}	-3^{11}	x^6+3x^3+3	
G_{24}	$-2^6 3^8$	x^6-3x^2+1	$\mathrm{Gal}(x^3-3x+1)=A_3$
$+S_4/V_4$	$2^6 229^2$	x^6-4x^2-1	$\mathrm{spl}(f)=\mathrm{spl}(x^4+x+1)$
S_4/Z_4	229^3	$x^6-3x^5+6x^4-7x^3+2x^2+x-4$	$\mathrm{spl}(f)=\mathrm{spl}(x^4+x+1)$
G_{36}^1	$2^8 3^9$	x^6+2x^3-2	
$+G_{36}^2$	$2^{10}3^6 5^4$	$x^6+6x^4+2x^3+9x^2+6x-4$	$f(x)=(x^3+3x+1)^2-5$
G_{48}	$-2^{11}5^2 7^2$	x^6+2x^2+2	
$+PSL_2(5)$	$2^{36}5^8$	$x^6+10x^5+55x^4+140x^3+175x^2+170x+25$	$\mathrm{spl}(f)=\mathrm{spl}(x^5+20x+16)$
G_{72}	$-2^8 733$	$x^6+2x^4+2x^3+x^2+2x+2$	$f(x)=(x^3+x+1)^2+1$
$PGL_2(5)$	$5^{20}19^3 151^3$	$x^6+10x^5+55x^4+140x^3+175x^2-3019x+25$	$\mathrm{spl}(f)=\mathrm{spl}(x^5-x+1)$
$+A_6$	$2^{16}3^6 5^6$	$x^6+24x-20$	
S_6	-101.431	x^6+x+1	
Degree 7			
$+Z_7$	$17^2 29^6$	$x^7+x^6-12x^5-7x^4+28x^3+14x^2-9x+1$	$\mathrm{spl}(f)=Q(z_{29}+z_{29}^{12}+z_{29}^{-1}+z_{29}^{-12})$
D_7	$-3^6 7^9$	$x^7+7x^3+7x^2+7x-1$	
$+F_{21}$	$2^6 7^{10}$	$x^7-14x^5+56x^3-56x+22$	
F_{42}	$-2^6 7^7$	x^7+2	
$+PSL_3(2)$	$7^8 17^2$	$x^7-7x^3+14x^2-7x+1$	
$+A_7$	$3^6 7^8$	$x^7+7x^4+14x+3$	
S_7	$-11.239.331$	x^7+x+1	

Given G, to find monic integral $f(x)$ such that $\mathrm{Gal}(f) = G$, where it is nontrivial to construct an appropriate splitting field, we do computer searching. If G is a group of even permutations, we first seek f such that $\mathrm{disc}(f)$ is a square. We also search for f such that, for all primes p in a fixed set, either $p|\mathrm{disc}(f)$ or the degree partition of $f \bmod p$ is the cycle type of some permutation in G.

There has recently been interest in polynomials with $PSL_3(2)$ as Galois group over Q [5, 8, 15]. The new example in Table II has the property that its discriminant, $7^8 17^2$, is the smallest discriminant of any monic integral polynomial with Galois group $PSL_3(2)$ over the rationals of which the authors are aware. We are unable to determine if this example fits into LaMacchia's [8] parametric family.

REFERENCES

1. W. E. H. BERWICK, On soluble sextic equations, *Proc. London Math. Soc. (2)* **29** (1929), 1–28.
2. G. BUTLER AND J. MCKAY, The transitive groups of degree up to 11, *Comm. Algebra* **11** (1983), 863–911.
3. J. J. CANNON, Software tools for group theory, *in* AMS Proc. Sympos. Pure Math. No. 37, pp. 495–502, 1980.
4. E. DEHN, "Algebraic Equations" (reprint), Dover, New York, 1960.
5. D. W. ERBACH, J. FISCHER, AND J. MCKAY, Polynomials with PSL (2, 7) as Galois group, *J. Number Theory* **11** (1979), 69–75.
6. H. O. FOULKES, The resolvents of an equation of the seventh degree, *Quart. J. Math. Oxford Ser. (2)* (1931), 9–19.
7. J. C. LAGARIAS AND A. M. ODLYZKO, Effective versions of the Chebotarev density theorem, *in* "Algebraic Number Fields (L-functions and Galois properties)" (A. Frohlich, Ed.), pp. 409–464, Academic Press, London, 1977.
8. S. E. LAMACCHIA, Polynomials with Galois group PSL(2, 7), *Comm. Algebra* **8** (1980), 983–992.
9. P. LEFTON, Galois resolvents of permutation groups, *Amer. Math. Monthly* **84** (1977), 642–644.
10. J. MCKAY, Some remarks on computing Galois groups, *SIAM J. Comput.* **8** (1979), 344–347.
11. G. B. MATHEWS, "Algebraic Equations," Cambridge Univ. Press, London, 1930.
12. I. R. SHAFAREVICH, Construction of fields of algebraic numbers with given solvable Galois group, *Izv. Akad. Nauk SSSR Ser. Mat.* **18** (1954), 525–578.
13. L. SOICHER, "The Computation of Galois Groups," Master's thesis, Concordia University, Montreal, 1981.
14. R. P. STAUDUHAR, The determination of Galois groups, *Math. Comp.* **27** (1973), 981–996.
15. W. TRINKS, Ein Beispiel eines Zahlkörpers mit der Galoisgruppe PSL(3, 2) über Q, manuscript, Universität Karlsruhe, 1968.
16. B. L. VAN DER WAERDEN, "Modern Algebra," Vol. 1 (transl. by F. Blum), Ungar, New York, 1953.
17. H. ZASSENHAUS, On Hensel factorization, I, *J. Number Theory* **1** (1969), 291–311.